REMARKS

Claims 1-14, 16 and 17 are pending in the Application and are now presented for examination. Claims 1-6, 8-14, 16 and 17 have been amended. Claim 15 has been cancelled, without prejudice and without disclaimer of subject matter. No new matter has been added.

Claims 1, 6, 11, 16 and 17 are independent.

Patentability under 35 U.S.C. §112

On page 2 of the Office Action, Claims 1, 3, 6, 8 and 11 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant has amended the claims to replace the phrase 'potentially not trusted' with the word 'suspect' as suggested by the Examiner. Applicant believes the amendment overcomes the rejections and respectfully request the rejections to these claims be withdrawn.

Patentability under 35 U.S.C. §103

On page 3 Claims 1-14, 16 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No.: 6,141,778, issued to Kane *et al.* ("Kane") in view of U.S. Patent: 6,718,386 B1, issued to Hanfland ("Hanfland"). Applicant respectfully traverses. Applicant asserts that neither Kane nor Hanfland, whether considered separately or in combination, teach, disclose or suggest the features of amended independent Claim 1.

Independent Claim 1

A feature of amended independent Claim 1 recites "compar[ing] each member within the group to a first list, the first list including names of ***trusted individuals authorized to perform system administrator tasks***," "determine whether the group includes at least one suspect member

not on the first list, and if so, generate a report identifying said at least one ***suspect*** member," and third program instructions that "determine whether the group has a group name on a second list of group names generally used for a group with untrusted user level privilege." These features are not taught, disclosed or suggested by Kane or Hanfland, either standing alone or in combination.

Neither Kane nor Hanfland teach, disclose or suggest a "first list including names of trusted individuals authorized to perform system administrator tasks"

As an initial matter, the Office Action does not cite Hanfland to teach, disclose or suggest the above features of amended Claim 1. Kane also does not teach, disclose or suggest these features. The Office Action relies on FIGs. 7 and 8 of Kane to show a list of trusted individuals, specifically relying on the HR_DATA and the CONTRACTOR _DATA tables. However, these tables merely contain the names of all employees and contractors. Col. 5, ll. 31-33, ll. 51-52. The people mentioned in these tables are not trusted individuals who can perform system administrator tasks. For at least this reason, Applicant respectfully asserts that amended Claim 1 is patentable over Kane and Hanfland, whether considered alone or in combination.

Neither Kane nor Hanfland teach, disclose or suggest "determine whether the group includes at least one suspect member not on the first list" of trusted individuals authorized to perform system administrator tasks

As an initial matter, the Office Action does not cite Hanfland to teach, disclose or suggest the above features of amended Claim 1. Kane also does not teach, disclose or suggest these features. The Office Action relies on FIG. 5 to show instructions to determine whether the group includes at least one member not on the first list. However, in FIG. 5 Kane merely shows the

algorithm used in "updating the security database" with data from other databases. Col. 8, ll. 7-9. "The RACF databases 22-28 are unloaded … [and] the unloaded data from the RACF databases 22-28 populates the … security database 30." Col. 8, 11-16. Also, "the human resources database 132 … populates … the security database 30. Similarly, in step 150, the … contractor services database 134 … populate[s] … the security database 30 in step 152. In step 154 the security system imports organizational data from the general ledger 130, and … populate[s] … the security database 30." Col. 8, ll. 16 -28. This is done periodically to update the security database. Col. 8, ll. 7-9. The data from the human resources database, from the contractor services database and from the general ledger is used "to verify the accuracy of the data loaded" from the RACF databases 22-28, but not to compare the members against a list of trusted individuals who are authorized to perform system administrator tasks. Col. 8, ll. 32-37.

Kane's system simply updates database fields for all individuals in the security system, both employees and contractors. While Kane may update a field in a database, Kane is not concerned about whether an individual assigned to a group is an ***untrusted suspect*** individual. In fact, Kane does not check at all whether an individual is trusted because Kane just updates one database with data from another one. Kane checks whether the security database fields for **all** the users in the security database are consistent with the RACF database fields for **all** the users in the RACF database. Checking consistency between databases is different from determining whether a member already in a group is a trusted member.

In fact, Kane suffers from the very problem the present invention is trying to solve, because nowhere does Kane check if a user in a group ***should be*** in the group assigned. An untrusted user in Kane may have been erroneously assigned to a group that should only have

members that are trusted individuals. Because Kane does not determine whether the data entered in the databases contain an untrusted user assigned to a trusted group that should only contain members that perform system administrator tasks, Kane will not realize that a suspect member exists in a group. Kane does not determine whether a group includes an untrusted member, as nothing in Kane shows a list of trusted individuals that can be used to find suspect members. Simply updating the RACF database to be consistent with data from another database is very different from determining if the group includes a suspect member not on a list of trusted individuals. For at least this additional reason, Applicant respectfully asserts that amended Claim 1 is patentable over Kane and Hanfland, whether considered alone or in combination.

Neither Kane nor Hanfland teach, disclose or suggest "generate a report identifying said at least one suspect member not on the first list"

As an initial matter, the Office Action does not cite Hanfland to teach the above features of amended Claim 1. Kane also does not teach, disclose or suggest the above features of Claim 1. Kane does not show a report identifying a member that is not on a list of trusted individuals authorized to perform ***system administrator tasks***. The Office Action relies on Figs. 4, 7 and 8 to show the above feature of amended Claim 1. However, Kane merely shows that "[t]he system provides for multiple reporting functions." Col. 2, ll. 50-51. In the description of FIG. 4, Kane shows "[t]he administrators 138 also receive reports generated by the security system 11" and that "security personnel ... [has] access to information, reports and control over the security system." Col. 7, ll. 60-61 and Col. 8, ll. 3-4. Nevertheless, Kane does not show a reporting function identifying a member that is not a system administrator. Regarding FIG. 7, Kane merely shows assigning a user id to an individual employee who does not have a current user id,

and displaying a message if the employee's status is inactive. Because the user in Kane does not have a current user id, the user might not even be a member of any group. "FIG. 7 shows an exemplary embodiment of the steps performed by the administrators 138 in periodically assigning a user identifier to an employee." Col. 9, ll. 1-3. The "administrator enters the employee's social security number," (Col. 9, ll. 4-5) and, "[i]f the employment status is inactive, then in step 172 the security system 11 displays a message telling the administrator 138 that the employee is on inactive status and may not be assigned a user identifier." Col. 9, ll. 12-16. Otherwise, "a new user identifier" is generated. Col. 9, ll. 31-32.

Kane waits for an administrator to manually enter an employee's social security number to check the employee's status, and if the employee has an inactive status, a message is displayed. This is very different from going through each member of a group and comparing each member against a list of trusted individuals, and "generat[ing] a report" identifying a suspect member. Kane does not check a group for members ***already in the group*** that should **not** be in the group. Regarding FIG. 8, Kane shows "shows an exemplary embodiment of the steps performed by the administrators 138 in periodically assigning a user identifier to a contractor." Col. 9, ll. 54-55. If "the contractor has been terminated … the security system 11 displays a message telling the administrator 138 that the contractor is terminated and may not be assigned a user identifier." Again, Kane does not identify a suspect member who is not on the list of system administrators. For at least this additional reason, Applicant respectfully asserts that amended Claim 1 is patentable over Kane and Hanfland, whether considered alone or in combination.

Neither Kane nor Hanfland teach, disclose or suggest "determin[ing] whether the group has a group name on a second list of group names generally used for a group with user level privilege, and if so, generate a report indicating that the group has a group name generally used for a group having user level privilege, such that members of the group are revealed as suspect."

As an initial matter, the Office Action does not cite Kane as teaching, disclosing or suggesting the above features of amended Claim 1. Hanfland also does not teach, disclose or suggest the above features of Claim 1. The Office Action relies upon Hanfland to teach these features. In support of this position, the Office Action cites to user labels 50 in FIGs. 3 and 4. Applicant respectfully disagrees with this characterization. Hanfland shows a list of **all** users and not a list of group names "used for a group with untrusted user level privilege." "FIG. 3 is an exemplary view of a display 42 of a three-dimensional view of privilege state data." Col. 7, ll. 64-65. "The user labels [50] in FIG. 3 include "Public", "Default", "CEO" and "JoeUser". The "Public" label corresponds to a public group and is used to set privileges for objects that are available to all users of the network system 10. The "Default" label corresponds to a default user group and is used to set privileges if no privilege state data is set for corresponding objects and privileges for a user group(s) or user(s). The "CEO" label is a representative label for a group of users of the network system 10. The "JoeUser" label applies to a user of the network system 10." Col. 9, ll. 56-65.

The Office Action relies on user labels 50 and FIGs. 8 and 11 to show a "second list of group names generally used for a group with untrusted user level privilege," and generate a report "such that members of the group are revealed as suspect." However, Hanfland clearly

states that FIG. 11 is a list of **all** the groups and users in the system. "FIG. 11 is a view of a DISPLAY_TABLE that has four columns of associated data. The USER/GROUP_ID column stores the user data for **all** groups and users of the network system 10." Col. 13, ll. 8-11. Also FIG. 11 shows users having all different kinds of privileges and not just "user level privilege." For example, the CEO label has administration read and write privileges and addresses read and write privileges, but the public group has none of these privileges. Similarly, FIG. 8 shows **all** the groups in the system, "FIG. 8 is a view of the GROUP_TABLE and has five columns of associated data. The GROUP_ID column uniquely identifies **the groups** of user entities **in the network system** 10." Col. 12, ll. 17-20. FIG. 8 of Hanfland does not show a list of groups "with untrusted user level privilege," but shows all the groups in the system. Moreover, FIG. 8 is not a report revealing members as suspect, as FIG. 8 simple identifies the groups in the system. Nothing in Hanfland "determines whether the group has a group name … used for a group with untrusted user level," as Hanfland does not check to see if a group's name is a name that is commonly given to an untrusted group. For at least this additional reason, Applicant respectfully asserts that amended Claim 1 is patentable over Kane and Hanfland, whether considered alone or in combination.

Neither Kane nor Hanfland, whether considered separately or in combination, teach, disclose, or suggest "first program instructions to compare each member within the group to a first list, the first list including names of trusted individuals authorized to perform system administrator tasks; second program instructions to determine whether the group includes at least one suspect member not on the first list, and if so, generate a report," and "third program instructions to determine whether the group has a group name on a second list of group names

generally used for a group with untrusted user level privilege, and if so, generate a report" as recited in amended Claim 1. Applicant asserts that amended Claim 1 is patentable over Kane and Hanfland, whether considered separately or in combination, and respectfully requests the withdrawal of this rejection.

Claims 6, 11, 16 and 17

Claims 6, 11, 16 and 17 recite features similar to Claim 1. Specifically, Claim 6 recites the features of a "first list including names of trusted individuals authorized to perform system administrator tasks," "determining whether the group includes at least one suspect member not on the first list, and if so, generating a report," and "determining whether the group has a group name on a second list of group names generally used for a group with untrusted user level privilege, and if so, generating a report." In addition, Claim 6 has been amended to place the claim in better form by amending the claim to recite "a central processing unit, a computer readable memory and a computer readable storage media." Support for this amendment can be found at least in page 4, ll. 1-2; page 7, ll. 2-10; page 8, ll. 18-30; and page 9, ll. 13-14 of the Specification.

Claim 11 recites the features of a "first list including names of trusted individuals authorized to perform system administrator tasks," "determine whether the group includes at least one suspect member not on the first list, and if so, generate a report," and "determine whether the group has a group name not on a second list of group names generally used for a group having a privilege level higher than user level privilege, and if so, generate a report."

Claim 16 recites the features of "determin[ing] that a group with an actual privilege level higher than untrusted user level privilege has a group name on a list of group names generally

used for a group with untrusted user level privilege," "compar[ing] members of said group to a list of trusted individuals authorized to perform system administrator tasks, and if any suspect member of said group does not appear on said list of trusted individuals, remove said suspect member from said group."

In addition, Claim 6 has been amended to recite the features of "a central processing unit, a computer readable memory and a computer readable storage media." Support for this amendment can be found at least at page 4, ll. 1-2; page 7, ll. 2-10; page 8, ll. 18-30; and page 9, ll. 13-14 of the specification.

Claim 17 recites the features of "determin[ing] that a group with an actual privilege level higher than user level privilege has a group name not on a list of group names generally used for a group with privilege level higher than user level privilege," "compare members of said group to a list of trusted individuals authorized to perform system administrator tasks, and if any suspect member of said group does not appear on said list of trusted individuals, lower the actual privilege level of said group." As discussed above with respect to Claim 1, these features are not taught, disclosed or suggested by Kane or Hanfland, whether considered alone or in combination. These claims are therefore believed patentable, and Applicant respectfully requests the rejections to these claims be withdrawn.

Dependent Claims 2-5, 7-10 and 12-14

Claims 2-5, 7-10 and 12-14 are each dependent directly from one or another of independent Claims 1, 6, and 11 discussed above. These claims recite additional limitations which, in conformity with the features of their corresponding independent claim, are not disclosed or suggested by the art of record. The dependent claims are therefore believed

patentable. However, the individual reconsideration of the patentability of each claim on its own merits is respectfully requested.

For all of the above reasons, the claim objections are believed to have been overcome placing Claims 1-14 and 16-17 in condition for allowance, and reconsideration and allowance thereof is respectfully requested.

The Examiner is encouraged to telephone the undersigned to discuss any matter that would expedite allowance of the present application.

The Commissioner is hereby authorized to credit overpayments or charge payment of any additional fees associated with this communication to Deposit Account No. 090457.

Respectfully submitted,

Date: April 16, 2009

By: /Alan M. Weisberg/

Alan M. Weisberg
Reg. No.: 43,982
Attorney for Applicant
Christopher & Weisberg, P.A.
200 East Las Olas Boulevard, Suite 2040
Fort Lauderdale, Florida 33301
Customer No. 68786
Tel: (954) 828-1488
Fax: (954) 828-9122
email: ptomail@cwiplaw.com

139948